



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

09/852,937

05/10/2001

David M. Blaker

9269-5

5828

20792

7590

02/06/2006

MYERS BIGEL SIBLEY & SAJOVEC
PO BOX 37428
RALEIGH, NC 27627

EXAMINER

LANIER, BENJAMIN E

ART UNIT

PAPER NUMBER

2132

DATE MAILED: 02/06/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/852,937	Applicant(s) BLAKER ET AL.	
	Examiner Benjamin E Lanier	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 18 January 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-3, 6-8, 16-18, 21, 27-29 and 32 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-3, 6-8, 16-18, 21, 27-29 and 32 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 10 May 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Amendment

1. Applicant's amendment filed 18 January 2006 amends claims 6, 21, and 32. Applicant's amendment has been fully considered and is entered.

Response to Arguments

2. Applicant's arguments filed 18 January 2006 have been fully considered but they are not persuasive. Applicant's argument that neither the nonvolatile memory nor the volatile memory shown in figure 1b of England is associated with the cryptographic accelerator is not persuasive because as stated by Applicant, the processor can use both the nonvolatile memory and the volatile memory and that would constitute an association.

3. Applicant's argument that England does not disclose an operand being loaded from the system memory to the local memory is not persuasive because England discloses a secure booting and program loading procedure a first key pair is loaded into volatile memory from the boot loader section of the nonvolatile memory (Col. 13, line 64 – Col. 14, line 2).

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Art Unit: 2132

5. Claims 1, 6, 16, 21, 27, 32 are rejected under 35 U.S.C. 102(e) as being anticipated by England, U.S. Patent No. 6,327,652. Referring to claims 1, 6, 16, 21, 27, 32, England discloses a digital rights management system wherein a user computer system contains a processor, cryptographic processor, nonvolatile memory, and volatile memory (Figure 1B), which meets the limitation of a host processor, cryptographic processor integrated circuit, system memory, and local memory. Wherein signing, encryption, decryption, and authentication operations can be performed by the cryptographic processor (Col. 7, lines 44-50). As known to those of ordinary skill in the art, the nonvolatile memory (Figure 1B, 144) is the random access memory module discussed in England (Col. 6, lines 13-15) and would be the operational memory for the central processing unit (Figure 1B, 140). In a secure booting and program loading procedure a first key pair is loaded into volatile memory from the boot loader section of the nonvolatile memory (Col. 13, line 64 – Col. 14, line 2), which meets the limitation of loading at least one operand from the system memory to the local memory. Once loaded into the volatile memory, the private key of the first key pair is used to sign a boot log (Col. 14, lines 5-6). This procedure would be performed by the cryptographic processor and the results would of course be stored in the volatile memory, which meets the limitation of executing an instruction using the cryptographic process that references the at least one operand using a first relative position in the local memory, generating a result based on the at least one operand, and storing the result at a second relative position in the local memory. Since the private key is stored in the volatile memory it would have a relative position within that memory. The first key pair was never deleted, and therefore still exists within the volatile memory. So when the result of the signing operation is stored in volatile memory, it would have a different location in the volatile memory, which meets

Art Unit: 2132

the limitation of wherein the first relative position comprises a first offset from a base address in the local memory, and the second relative position comprises a second offset from the base address in the local memory. The processor can use both the nonvolatile memory and the volatile memory and that would constitute an association.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

8. Claims 2, 17, 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over England, U.S. Patent No. 6,327,652. Referring to claims 2, 17, 28, in addition to the above teachings, England discloses that after the first key pair is stored in volatile memory, a second key pair is stored in volatile memory (Col. 14, lines 3-5). The second private key from the second key pair is later used to sign the boot log (Col. 14, lines 12-14), which meets the limitation of executing the instruction using the cryptographic processor that references a first one of the operands using the first relative position in the local memory and a second one of the operands using a second

Art Unit: 2132

relative position in the local memory. England does not disclose exactly where in memory the key pairs are stored, but it would have been obvious to one of ordinary skill in the art at the time the invention was made for the key pairs to be stored contiguous to one another since the memory is volatile and the operations are being performed subsequent to a boot operation (Col. 11, lines 39-45). After the boot operation the volatile memory would be empty, and therefore subsequent data stored within would be stored contiguously.

9. Claims 3, 18, 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over England, U.S. Patent No. 6,327,652, in view of Schneier. Referring to claims 3, 18, 29, England discloses storing multiple key pairs and signing a boot log with the private keys (Col. 13, line 60 – Col. 14, line 14), but does not disclose that the keys are different sizes. It would have been obvious to one of ordinary skill in the art at the time the invention was made because England discloses that the private keys are valid for a short duration of time (Col. 15, lines 39-47) and a wise cryptographer would determine the length of the key based on the lifetime of the key (Schneier, page 160). Since the key pairs correspond to different components, it would be understood that the lifetime of the keys would be different for different components.

Conclusion

10. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

Art Unit: 2132

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

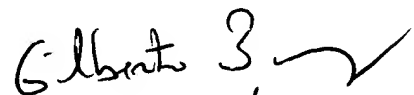
11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin E. Lanier whose telephone number is 571-272-3805. The examiner can normally be reached on M-Th 7:30am-5:00pm, F 7:30am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Benjamin E. Lanier



GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100